UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/667,010	09/21/2000	Uve Hansmann	IBM-116	8803

7590 01/19/2006

Thomas A Beck
26 Rockledge Lane
New Milford, CT 06776

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/667,010	HANSMANN ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 3 October 2005.

2. Claims 1-11 are pending in the application.

3. Claims 1-11 have been rejected.

Response to Arguments

4. Applicant's arguments with respect to claims 1-11 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4, 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al U.S. Patent No. 6,088,450 in view of Bauman et al U.S. Patent No. 6,898,711 B1.

As to claim 1, Davis et al discloses a method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising:

> the devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation [column 3 line 52 to column 4 line 11];

establishment of a link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, the encryption data being stored solely in the authentication system, the link between the authentication system and the device being via wired or wireless means [column 4, lines 12-19].

checking the encryption data in the authentication system prior to operation of the electronic device control [column 4, lines 12-19];

assignment of predetermined means of access to the electronic device control associated with the authentication system the predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, the software function evaluates a security token and is running on top of the physical hardware [column 5 line 50 to column 6 line 50];

enabling of the means for access predetermined for the authentication system dependent on the result of the check [column 5 line 50 to column 6 line 50].

Davis et al does not teach the method providing means of no access or full access and allow more finely defined levels of access as defined in a user profile for configuration or maintenance work.

Bauman et al teaches providing means of no access or full access and allows more finely defined levels of access as defined in a user profile [column 5 line 35 to column 6 line 65].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Davis et al so that the user would have had a profile configured for providing means of no access or full access and more finely defined levels of access.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Davis et al by the teaching of Bauman et al because the profile tokens represents users and may be used anytime a user would need to be authenticated. Since profile token have usage restrictions and a number of control mechanisms associated with hem, a compromised token may be viewed as a significantly lower security risk as compared to a compromised conventional user ID/password combination [column 4 line 60 to column 5 line 5].

As to claim 2, Davis et al teaches that the basic means of access to functions of the device comprise at least one of the following means: disable operation of the devices, enable operation of the devices, or enable configuration of the devices [column 5 line 50 to column 6 line 50].

As to claim 3, Davis et al teaches that the link is made without need for intermediate software layers [column 7, lines 35-62].

As to claim 4, Davis et al teaches in addition, the step of reading at least one of the following features embodied within the authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic [column 5, lines 34-49].

As to claim 10, Davis et al teaches program code areas for the execution or preparation for execution of the steps when the program is installed in a computer [column 5, lines 34-49].

As to claim 11, Davis et al discloses a method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising:

the devices comprising computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation [column 3 line 52 to column 4 line 11];

establishment of a link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, the encryption data being stored solely in the authentication system, the link between the authentication system and the device being via wired or wireless means [column 4, lines 12-19].

checking the encryption data in the authentication system prior to operation of the electronic device control [column 4, lines 12-19];

assignment of predetermined means of access to the electronic device control associated with the authentication system the predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, the software function evaluates a security token and is running on top of the physical hardware [column 5 line 50 to column 6 line 50];

enabling of the means for access predetermined for the authentication system dependent on the result of the check [column 5 line 50 to column 6 line 50].

Davis et al does not teach the method providing means of no access or full access and allow more finely defined levels of access as defined in a user profile for configuration or maintenance work.

Bauman et al teaches providing means of no access or full access and allows more finely defined levels of access as defined in a user profile [column 5 line 35 to column 6 line 65].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Davis et al so that the user would have had a profile configured for providing means of no access or full access and more finely defined levels of access.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Davis et al by the teaching of Bauman et al because the profile tokens represents users and may be used anytime a user would need to be authenticated. Since profile token have usage restrictions and a number of control mechanisms associated with hem, a compromised token may be viewed as a significantly lower security risk as compared to a compromised conventional user ID/password combination [column 4 line 60 to column 5 line 5].

6. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al U.S. Patent No. 6,088,450 and Bauman et al U.S. Patent No. 6,898,711 B1 as applied to claim 1 above, and further in view of Findikli et al U.S. Patent No. 6,415,144 B1.

As to claim 5, the Davis-Bauman combination does not teach that the method includes configuration of the devices, by authorized persons. The Davis-Bauman combination does not teach that after successful authentication, device-specific configuration data are downloaded into

the devices from the authentication system in accordance with the authentication systems or over a network.

Findikli et al teaches configuration of the devices, by authorized persons [column 1 line 61 to column 2 line 5]. Findikli et al teaches that device-specific configuration data are downloaded into the devices from the authentication system in accordance with the authentication systems or over a network [column 1 line 61 to column 2 line 5].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Davis-Bauman combination so that the method would have included configuration of the devices, by an authorized persons. After successful authentication, device-specific configuration data would have been downloaded into the devices from the authentication system in accordance with the authentication systems or over a network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Davis-Bauman combination by the teaching of Findikli et al because over-the-air teleservices provide the radio telecommunications system operators with greater flexibility in tailoring wireless devices to meet the needs of their subscribers [column 2, lines 6-10].

As to claim 6, the Davis-Bauman combination teaches execution setting basic means of access for operations [Davis et al column 6, lines 26-50].

As to claim 7, the Davis-Bauman combination teaches authentication of a person or a group of people [Davis et al column 6, lines 26-50].

As to claim 8, the Davis-Bauman combination teaches that the authentication system is implemented in the form of a Smartcard [Davis et al column 4, lines 20-28].

As to claim 9, the Davis-Bauman combination teaches setting basic means of access for operation of devices of which the operation is controllable by electronic means, including at least one device and an authentication system [Davis et al column 6, lines 26-50].

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
January 10, 2006

Primary Examiner
AU2131
1/13/06